FREQUENTIS
FOR A SAFER WORLD

Erfahrungsbericht: Security für Safety-kritische Leitzentralen

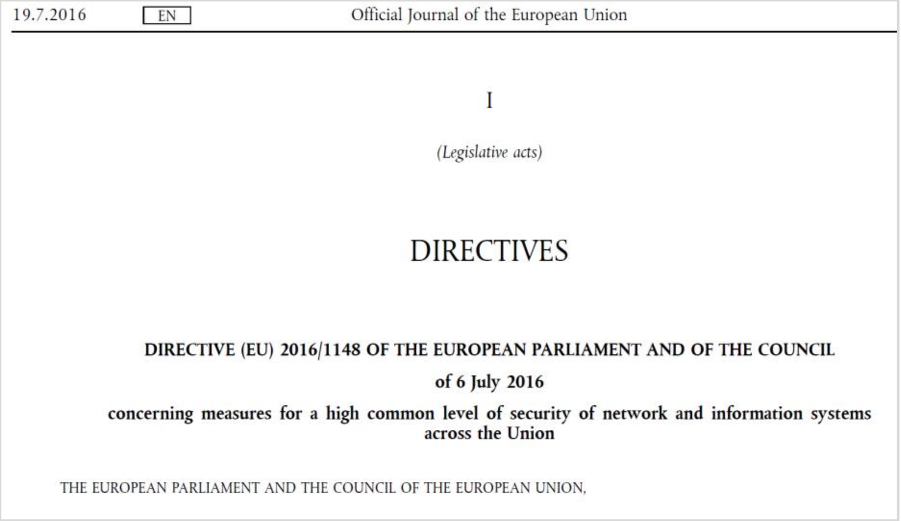
DI Dr. Christian Flachberger CISSP, CSSLP
DI Dr. Andreas Gerstinger CSSLP
DI Rainer Frischmann CSSLP

Highly reliable communication and information solutions for a safer world

70 years of innovation in safety-critical applications

We set standards

Neue Gesetze – Sorgfaltspflichten für Betreiber von Infrastrukturen



19.7.2016 EN Official Journal of the European Union

I

(Legislative acts)

DIRECTIVES

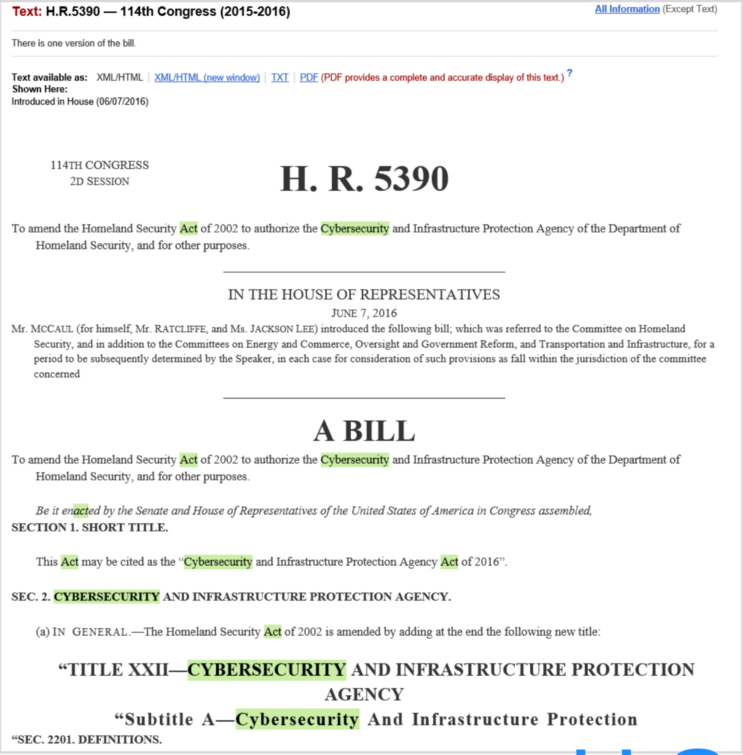
DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 6 July 2016

concerning measures for a high common level of security of network and information systems across the Union

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

EU



Text: H.R.5390 — 114th Congress (2015-2016) All Information (Except Text)

There is one version of the bill.

Text available as: XML/HTML | XML/HTML (new window) | TXT | PDF (PDF provides a complete and accurate display of this text.) ?
Shown Here:
Introduced in House (06/07/2016)

114TH CONGRESS
2D SESSION

H. R. 5390

To amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Protection Agency of the Department of Homeland Security, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

JUNE 7, 2016

Mr. MCCAUL (for himself, Mr. RATCLIFFE, and Ms. JACKSON LEE) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committees on Energy and Commerce, Oversight and Government Reform, and Transportation and Infrastructure, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To amend the Homeland Security Act of 2002 to authorize the Cybersecurity and Infrastructure Protection Agency of the Department of Homeland Security, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "Cybersecurity and Infrastructure Protection Agency Act of 2016".

SEC. 2. CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY.

(a) IN GENERAL.—The Homeland Security Act of 2002 is amended by adding at the end the following new title:

"TITLE XXII—CYBERSECURITY AND INFRASTRUCTURE PROTECTION AGENCY

"Subtitle A—Cybersecurity And Infrastructure Protection

"SEC. 2201. DEFINITIONS.

U.S.

Andrew Rose, head of cyber security at NATS,

London, April 2017

Drei Ursachen für mangelhafte Cybersicherheit:

- Mangelndes Verständnis und Know-how der Betreiber
- Konflikte zwischen Safety und Security best practises
- Schlecht absicherbare Produkte der Hersteller

Beispiele für Kundenanforderungen (aus Ausschreibungen)

1. **Patching times**

   “The supplier shall procure the ***application of security patches*** *to vulnerabilities within a maximum period from the public release of such patches with those vulnerabilities categorized as* ***'Critical 'within 14 days of release****, 'important' within 30 days of release and at 'Other' within sixty (60) Working Days of release“ (UK)*

   “Updates to ***remediate critical vulnerabilities*** *shall be provided within a shorter period than other updates****, within at least three (3) days****” (AUS)*

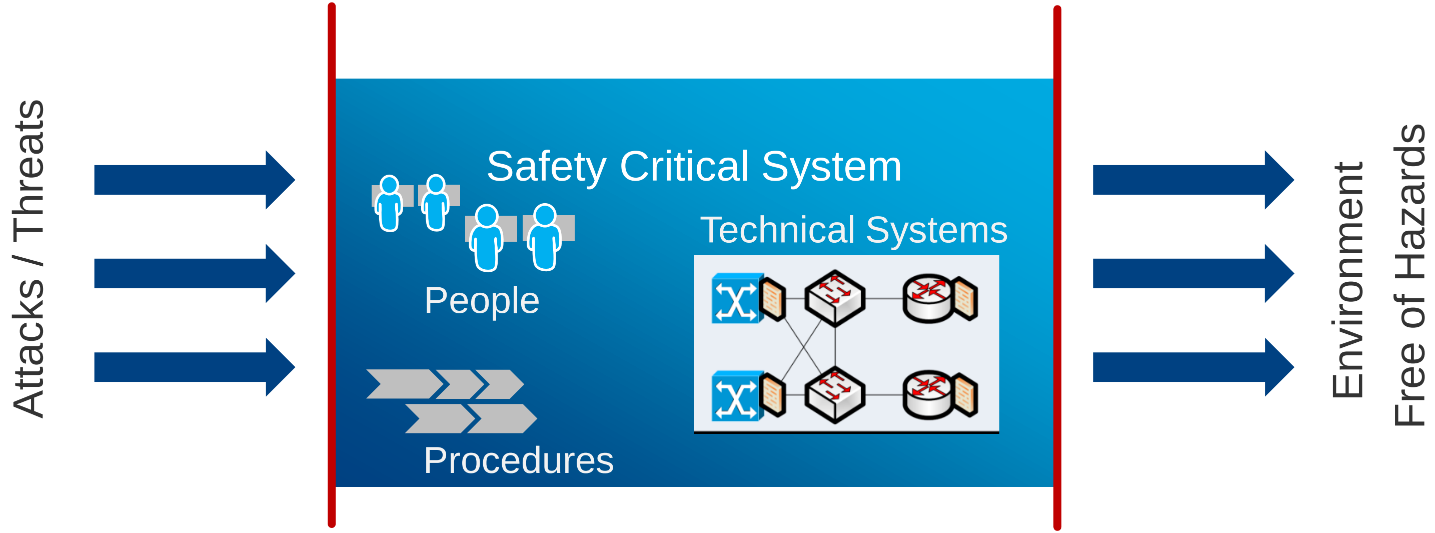
2. **Maintain the compatibility with patches**

   “The Supplier’s software maintenance shall include ***maintaining compatibility with operating system updates*** *(which will be* ***maintained on behalf of the Authority by others****)”. (UK)*

3. **A demonstrable supply chain security management and security services covering also third party components**

   *“****When third-party hardware, software, and firmware is procured by the Contractor****, the Contractor shall demonstrate that it has included arrangements[..] to* ***provide appropriate hardware, software, and firmware updates to remediate newly discovered vulnerabilities or weaknesses within one month*** *[...]. Updates to* ***remediate critical vulnerabilities shall be provided [...] within 3 days****. If these third-party updates cannot be made available by the vendor within these time periods, the Contractor shall provide* ***mitigations and/or workarounds within one week*** *[...].” (AUS)*

Managing Safety *and* Security



Security

protection against attacks

Safety

freedom from unacceptable risk of harm

Security impacts Safety

Safety has priority over Security

Can Safety and Security be Combined?

Common Safety and Security Approach

- Risk-based approach
- Identification and avoidance of hazards/threats
- Must be considered along the whole lifecycle
- Safety/Security awareness, culture and trainings
- Avoidance and detection of faults and failures/ vulnerabilities and incidents

- Risk-based approach
- Identification and avoid
- Must be considered along the whole lifecycle
- Safety awareness, culture and trainings
- Avoidance and detection of faults and failures

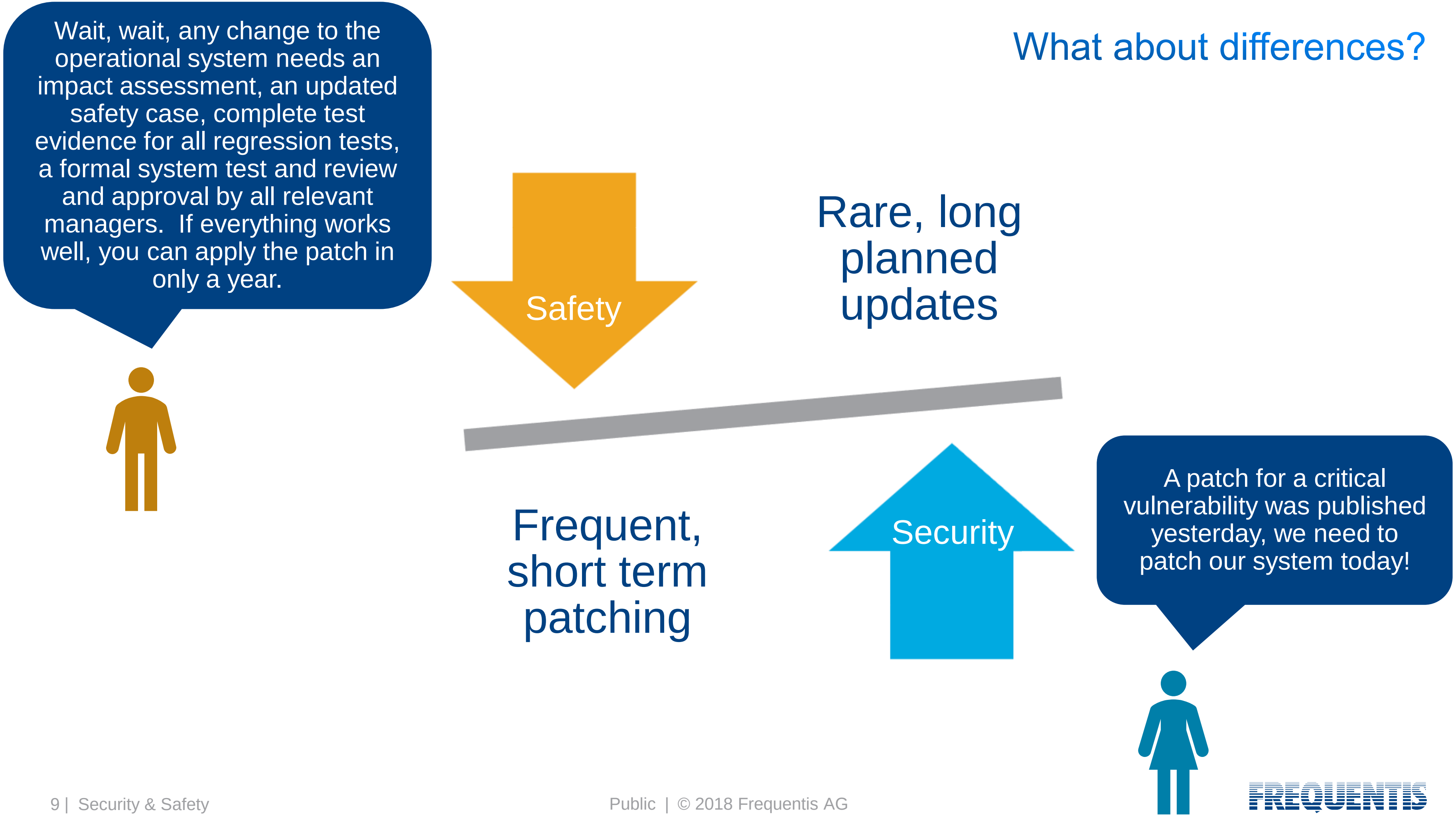
Safety

dance of threats

- Must be considered along the whole lifecycle
- Safety awareness, culture and trainings
- Avoidance and detection of vulnerabilities and incidents

Security

What about differences?



Wait, wait, any change to the operational system needs an impact assessment, an updated safety case, complete test evidence for all regression tests, a formal system test and review and approval by all relevant managers. If everything works well, you can apply the patch in only a year.

Safety

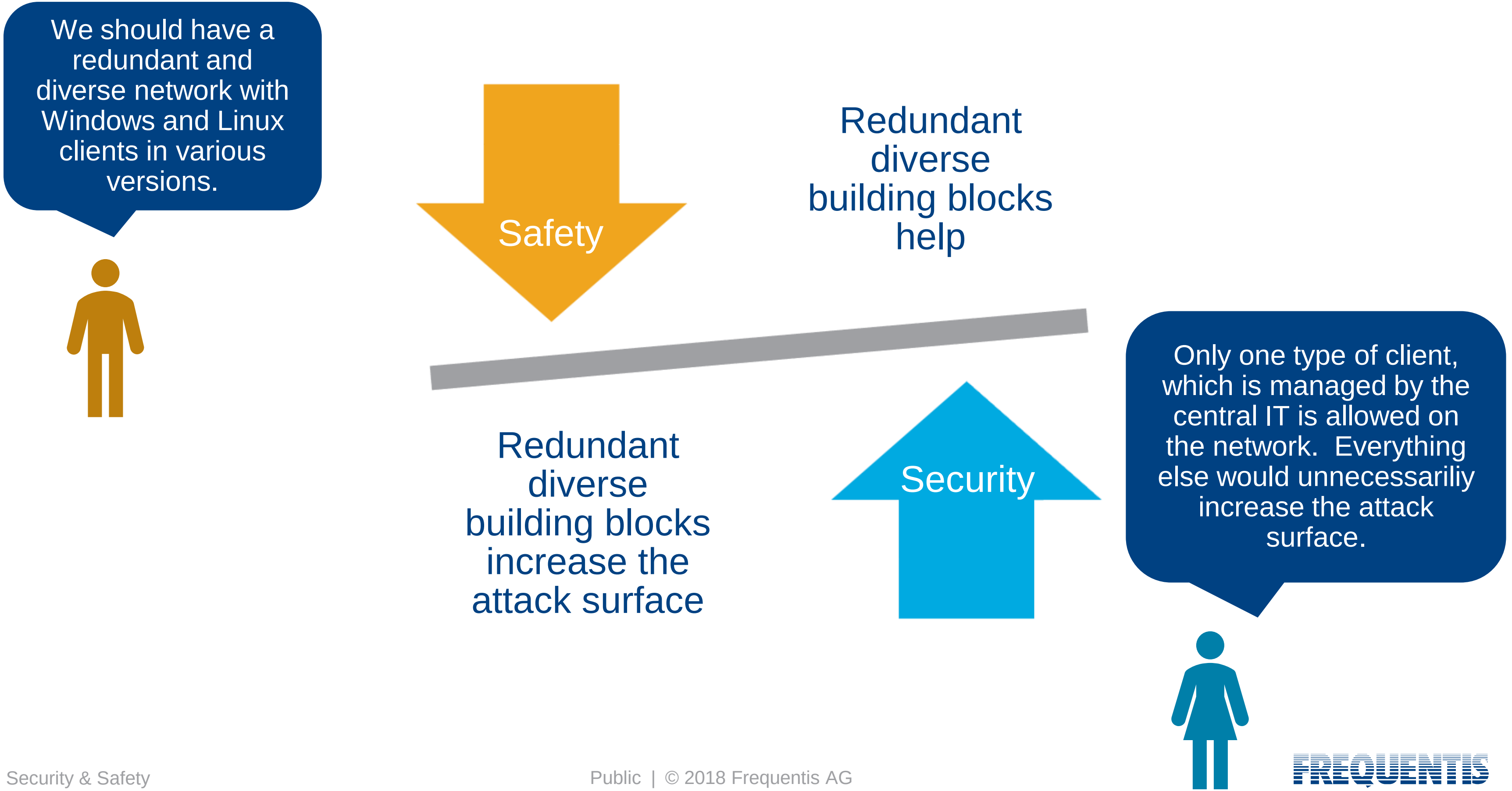
Rare, long planned updates

Frequent, short term patching

Security

A patch for a critical vulnerability was published yesterday, we need to patch our system today!

What about differences?



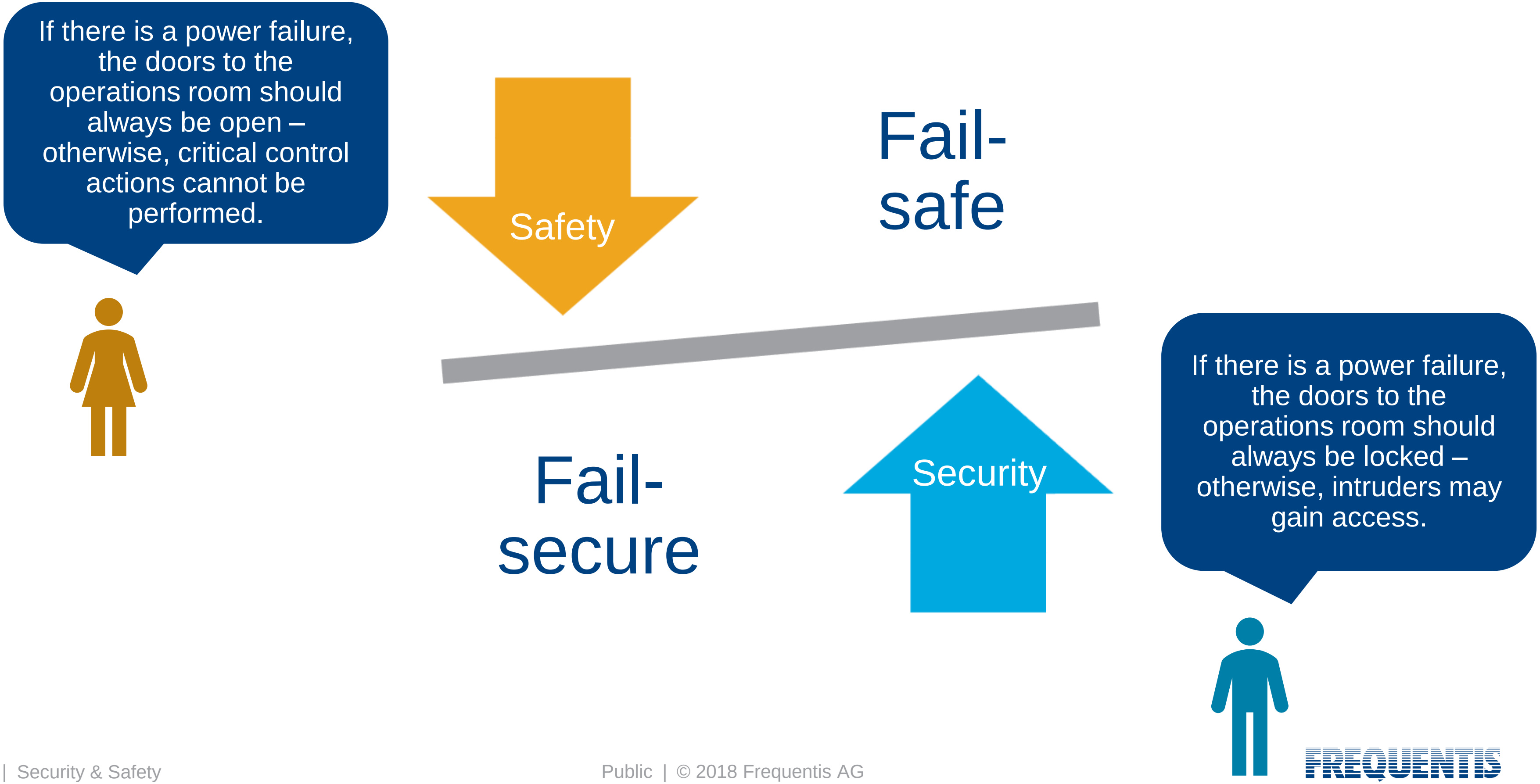
We should have a redundant and diverse network with Windows and Linux clients in various versions.

Redundant diverse building blocks help

Redundant diverse building blocks increase the attack surface

Only one type of client, which is managed by the central IT is allowed on the network. Everything else would unnecessariliy increase the attack surface.

What about differences?



If there is a power failure, the doors to the operations room should always be open – otherwise, critical control actions cannot be performed.

Safety

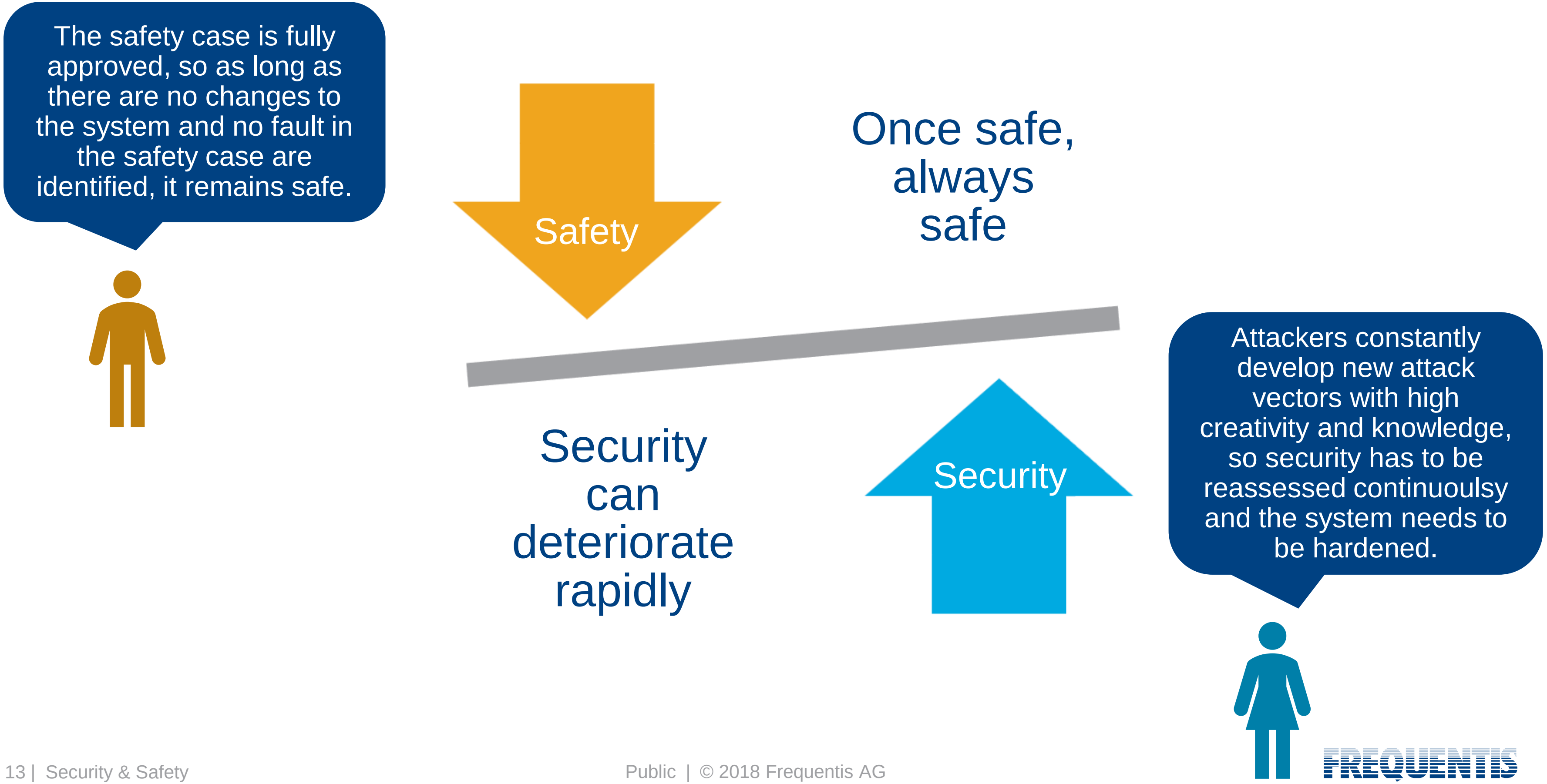
Fail-safe

Fail-secure

Security

If there is a power failure, the doors to the operations room should always be locked – otherwise, intruders may gain access.

What about differences?



The safety case is fully approved, so as long as there are no changes to the system and no fault in the safety case are identified, it remains safe.

Once safe, always safe

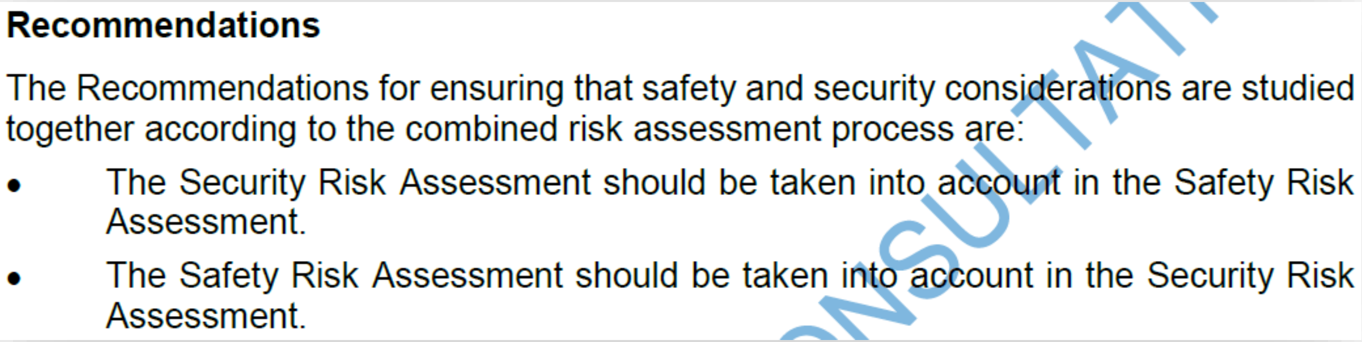
Security can deteriorate rapidly

Attackers constantly develop new attack vectors with high creativity and knowledge, so security has to be reassessed continuoulsy and the system needs to be hardened.

Common Safety and Security Approach

- Standards start to recognise that safety and security need to go together

- e.g. EUROCAE ED-205 (DRAFT). Process Standards for Security Certification/Declaration of Air Traffic Management/Air Navigation Services (ATM/CNS) Ground Systems.
  - "Decisions made about security must not compromise safety and vice-versa."
  - Harmonization of Processes

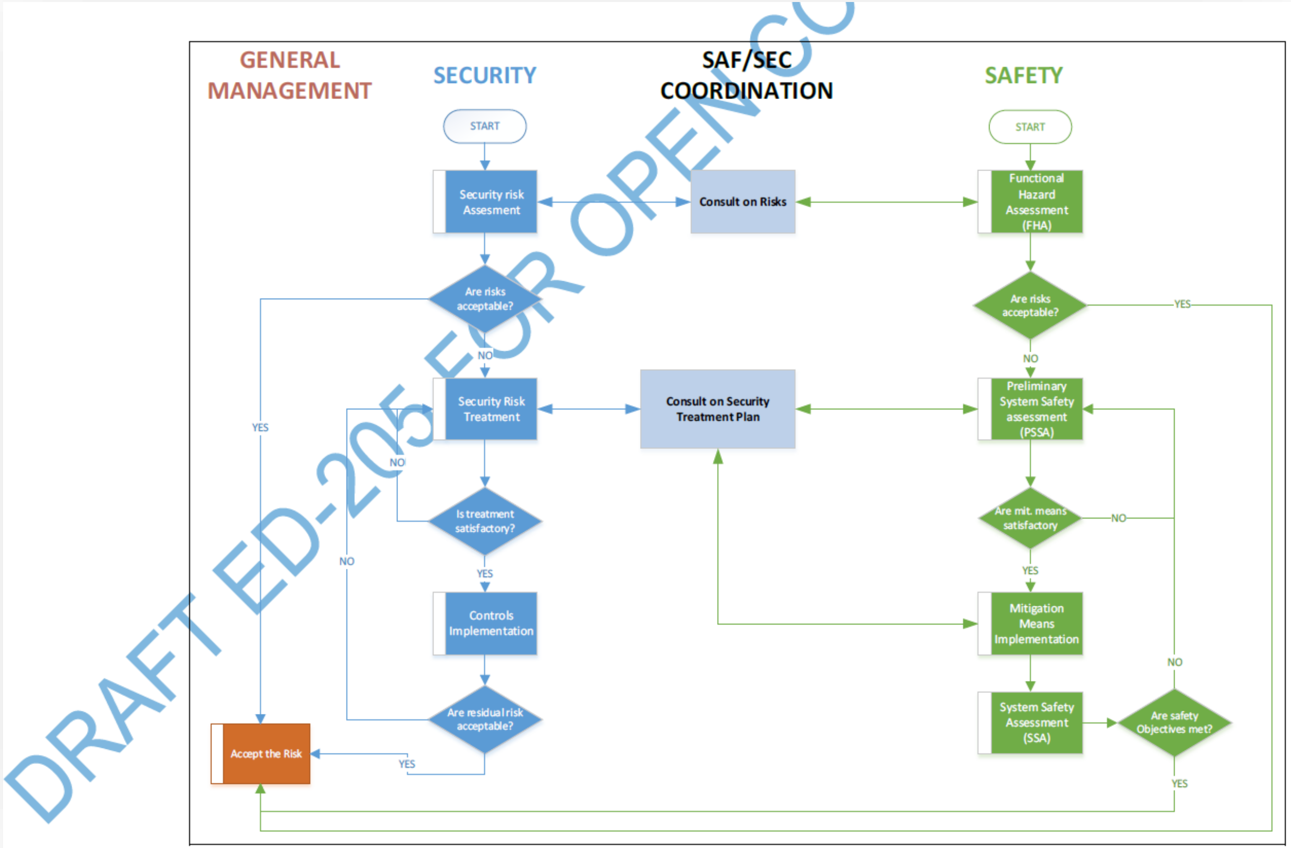


Recommendations

The Recommendations for ensuring that safety and security considerations are studied together according to the combined risk assessment process are:

- The Security Risk Assessment should be taken into account in the Safety Risk Assessment.
- The Safety Risk Assessment should be taken into account in the Security Risk Assessment.

Proposed Safety and Security Process (ED-205 DRAFT)



GENERAL MANAGEMENT

SECURITY

SAF/SEC COORDINATION

SAFETY

START

Security risk Assesment

Consult on Risks

START

Functional Hazard Assessment (FHA)

Are risks acceptable?

YES

NO

Security Risk Treatment

Consult on Security Treatment Plan

Are risks acceptable?

YES

NO

Preliminary System Safety assessment (PSSA)

NO

Is treatment satisfactory?

YES

NO

Are mit. means satisfactory

NO

YES

Controls Implementation

Mitigation Means Implementation

Are residual risk acceptable?

NO

System Safety Assessment (SSA)

Are safety Objectives met?

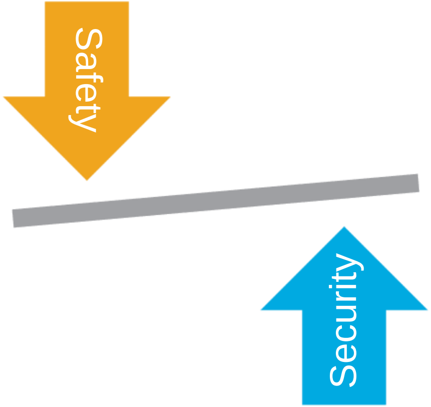
Accept the Risk

YES

YES

From the projects

Servant of two masters



- Logon
  - Security: complex passwords, auditing capabilities
  - Safety: immediate access to system for operators

- Patching
  - Security: patch, patch, patch
  - Safety: safety of the system must not be compromised, no changes, if there is a change you need to update the safety case

- Anti Virus
  - Security: current AV signatures, AV engine heuristics stops malicious programs
  - Safety: safety-critical programs and processes must not be stopped, the system has to be available 24/7

From the projects

Servant of two masters - Logon

Safety:
immediate access to system for operators

Security:
complex passwords, auditing capabilities

Reasoning:

- Complex passwords only for administrative accounts
- Strong physical security as mitigation for easy operator access
- Logging of logon/logoff for auditing by security staff
- Logon on unusual nodes creates security event in monitoring system

From the projects

Servant of two masters – patching 1

Safety:
safety of the system must not be compromised; no change; if there is a change you need to update the safety case

Security:
patch, patch, patch

Reasoning:

- Joint process involving all stakeholders
- Patches assessed against possible safety implications
- Patches only implemented after extensive structured testing to uphold safety case

From the projects

Servant of two masters – patching 2

Patching board

- Consists of Frequentis and several customer parties (operators, maintenance, security)
- Assess severity/necessity of patches
- Accept/reject patches

Different types of servers/nodes:

- Core servers: too risky and too expensive to patch
- Interface nodes: patching feasible

Patching:

- Normal patches within the normal maintenance cycle

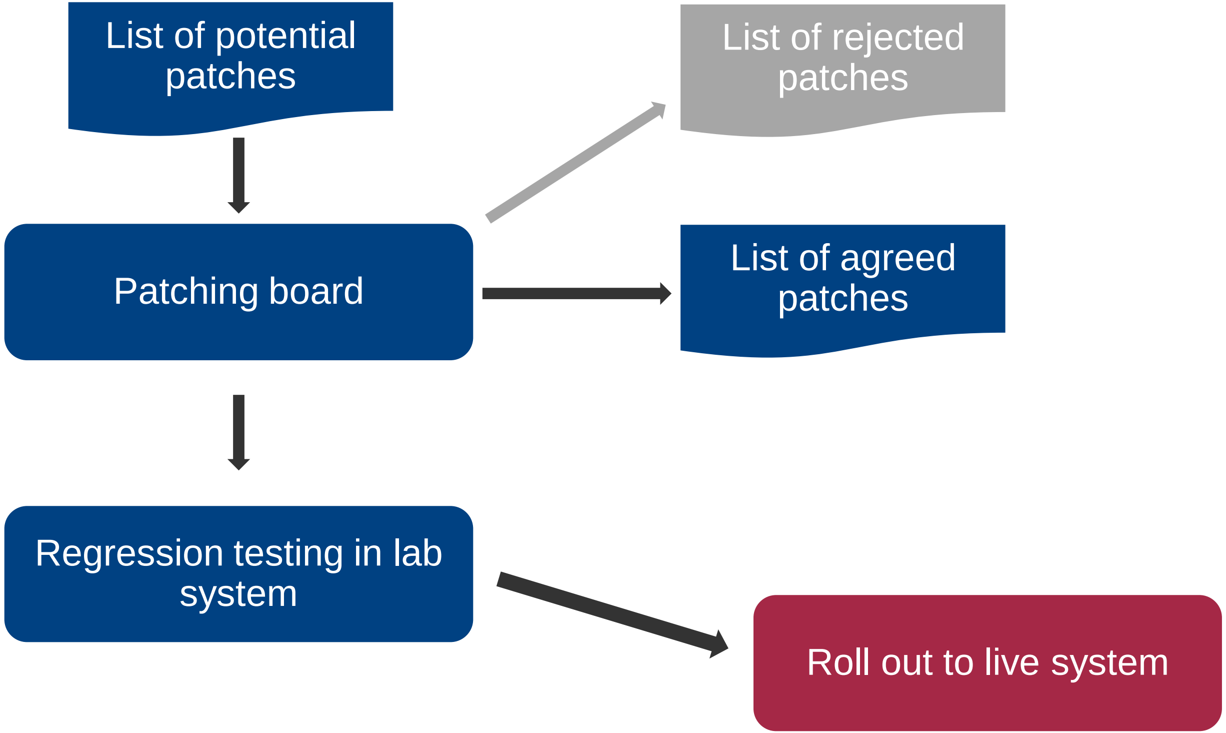
  → approx. 4-5 months for testing

- Critical patches within a shortened maintenance cycle

  → approx. 2 months for testing

From the projects

Servant of two masters – patching 3



List of potential patches

Patching board

List of rejected patches

List of agreed patches

Regression testing in lab system

Roll out to live system

From the projects

Servant of two masters – Anti Virus

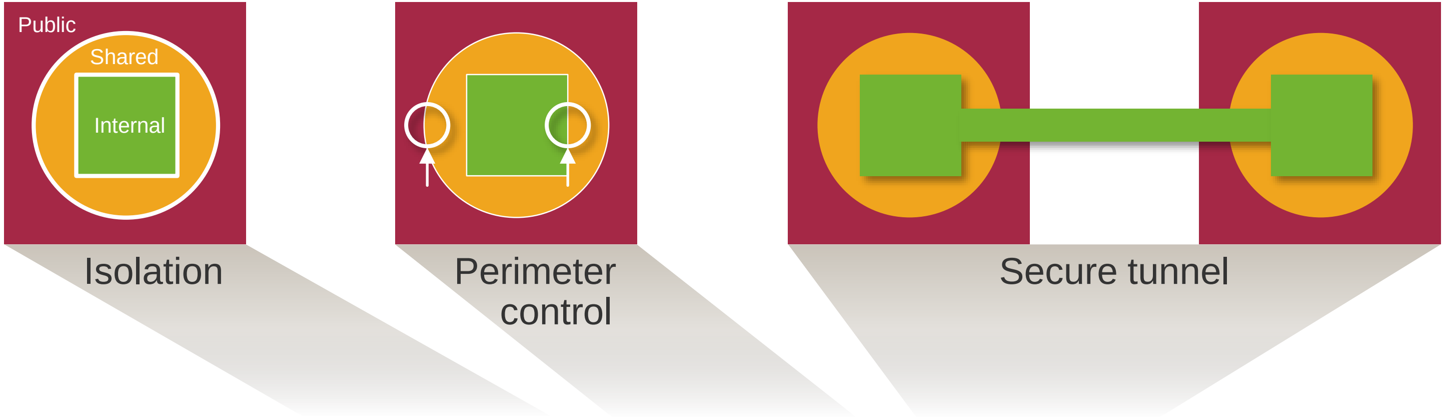
Safety:
safety-critical programs and processes must not be stopped, the system has to be available 24/7

Reasoning:

- Processes and services on core servers can‘t be stopped at will by Anti Virus software
- Core servers: too risky to put Anti Virus on
- Interface nodes: Anti Virus running and updated in a timely manner
- Sheep dip computers (https://en.wikipedia.org/wiki/Sheep_dip_(computing)) for exchanging data

Security:
current AV signatures, AV engine heuristics stops malicious programs

Integration of Safety and Security into a common system architecture



Protection zones

	Internal	Shared	Public
Safety criticality	High	Medium	Low
Connectivity to…	n/a	trusted networks	untrusted networks
Security concept	OT	OT / IT	IT

Information Technology

IT – Security

→ **Protect data**

C – I – A
Fail secure
IPS
Patches

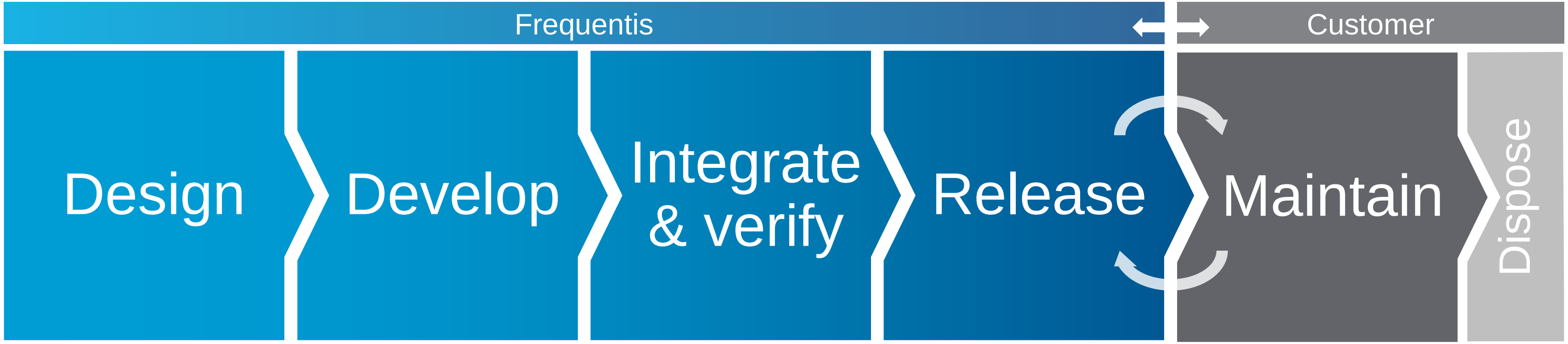
Operational Technology

OT – Security

→ **Protect processes**

A – I – C
Fail safe
IDS
SW assured revisions
Segmentation + Perimeter sec.

Security as process with a clear security responsibility in each phase



Frequentis Software Design Standard

Frequentis Software Coding Standard

Security verification by independent system security team

Formal security handover

Transition of responsibility

Security services

Security notifications

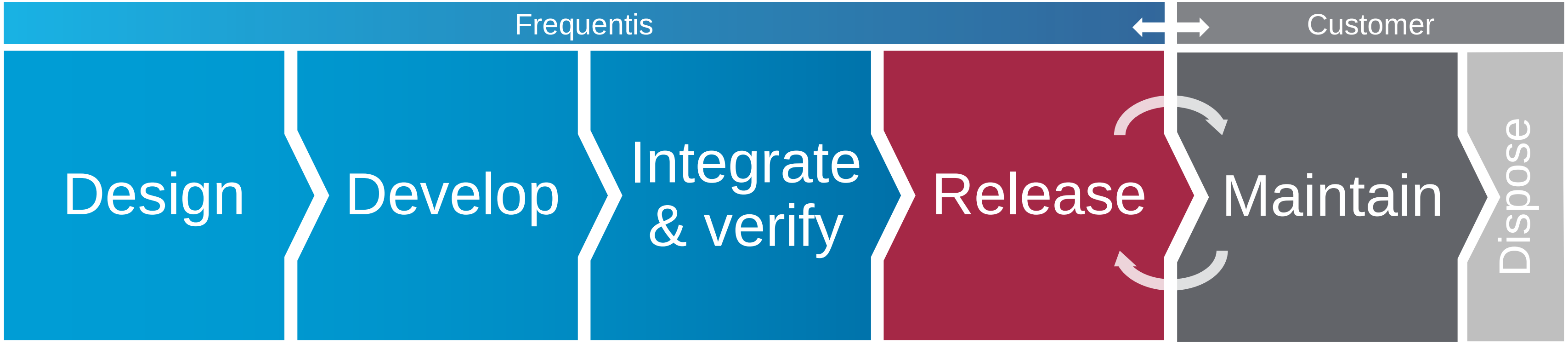
System monitoring

Patch provision

Security upgrades

Security incident response team (SIRT)

Security as process with a clear security responsibility in each phase



Frequentis

Customer

Design

Develop

Integrate & verify

Release

Maintain

Dispose

Frequentis Software Design Standard

Frequentis Software Coding Standard

Security verification by independent system security team

Formal security handover

Transition of responsibility

Security services

Security notifications

System monitoring

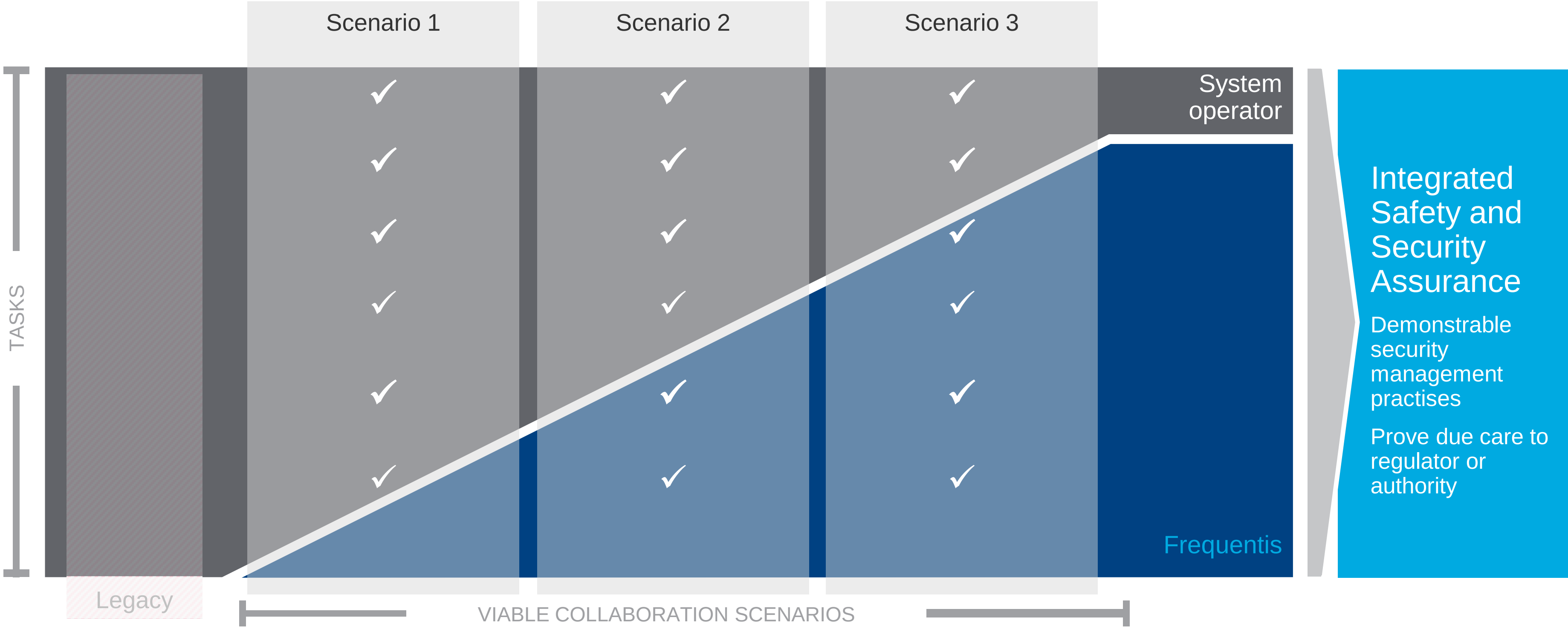
Patch provision

Security upgrades

Security incident response team (SIRT)

Security collaboration – sharing of duties

Common interest and collaborative effort of system operator, integrator and vendors



Integrated Safety and Security Assurance

Demonstrable security management practises

Prove due care to regulator or authority

FREQUENTIS

FOR A SAFER WORLD